2009

Cube-Type Algebraic Attacks on Wireless Encryption Protocols

Petrakos, Nikolaos

Computer 42:10 (2009), 103-105.
http://hdl.handle.net/10945/38853

CUBE-TYPE ALGEBRAIC ATTACKS ON WIRELESS ENCRYPTION PROTOCOLS

George W. Dinolt, James Bret Michael,

Nikolaos Petrakos, Pantelimon Stanica

Short-range (Bluetooth) and to so extent medium-range (WiFi) wireless networks are ubiquitous, being used in such places as the homes, hospitals, assembly lines, aircraft, and even wearable computers. Several types of attacks have been successful at defeating the cryptosystems used by IEEE 802.11 and 802.16 technologies, leading one to ask the question: how much trust should we place in the wireless encryption protocols?

In 2008 Dinur and Shamir proposed a type of algebraic attack called the *cube attack* [1] in which the active assault on a cryptosystem requires the attacker to extract useful information from the bit stream. By skillfully choosing some publicly settable bits, the attacker may be able to replace the degree of the polynomial that represents the encryption function by a system of linear equations. Dinur and Shamir used this approach on the Trivium cipher and recovered the encryption key in 2^{19} bit operations. The best attempt reported in the literature was that of Fischer, Khazaei and Meier [2] using chosen initialization vector (IV) statistical analysis and they succeeded in key recovery with a complexity of 2^{55} bit operations.

BLUETOOTH AND PREVIOUS ATTACKS

Bluetooth is a well-established wireless communications standard (IEEE 802.15.1) between different devices (e.g., personal computers, laptops, mobile phones) that operates over a short range and at low power. For efficiency reasons - speed, size and power consumption - the system uses the E0 (128 bit) stream cipher instead of one of the widely used block ciphers. In E0 cipher, four linear feedback shift registers (LFSRs) are used and a nonlinear Boolean

function combines their output. Combining the plaintext with the output key stream using an exclusive OR (XOR) produces the ciphertext.

Several attacks have been implemented on the Bluetooth system. In 2003, Armknecht and Krause [3] applied an *algebraic attack* on Bluetooth E0 (the idea of an algebraic attack is based on the ability of an attacker to solve a system of nonlinear multivariable equations of low degree). They recovered the key in $2^{68.48}$ operations after the adversary had knowledge of $2^{23.07}$ keystream bits. In 2004, Armknecht in [4] reduced the complexity at $2^{54.51}$ operations after the adversary had knowledge of $2^{23.44}$ keystream bits, by using a precomputation step. In 2004, Lu and Vaudenay [5] introduced a *fast correlation attack* by formulating a powerful computation method of correlations using a recursive expression based on the maximum likelihood decoding (MLD) algorithm using a fast Walsh transform (FWT). In order for their attack to succeed, they built a distinguisher for E0 based on the largest bias they found. Their best result for E0 is limited to 2^{37} operations. In 2005, Lu, Meier, and Vaudenay [6] proposed the *conditional correlation attack* which studies the linear correlation of the inputs conditioned on a known output pattern of a particular nonlinear function. The best result that they obtained on the E0 keystream generator required 24 bits of $2^{38.5}$ computations for key recovery.

CUBE ATTACK

The cube attack is a generic attack that may be applied to block ciphers, stream ciphers, or even keyed hash functions without necessarily having knowledge of the internal structure of the cipher, as long as at least one output bit can be represented by a polynomial of low degree of the secret and public variables. The foundation of the approach proposed by Dinur and Shamir is basic algebraic cryptanalysis, which involves attempting to lower the degree of the polynomial equations that represent a cryptosystem by polynomials of lower degree. They assume that the polynomial equations used to describe a cryptosystem are variants derived from a master polynomial by adding some

variables to any possible value. They call this attack the cube attack "...*since it sets some public variables to all their possible values in* n, $(d-1)$*-dimensional Boolean cubes, and sums the results in each cube*" (cf. [1]), where d represents the degree of the polynomial and n is the number of variables.

The cube attack may be completed in two phases: the *preprocessing phase,* where the attacker finds as many *maxterms* (a term or cube of the encryption function such that its co-factor is a linear nonconstant polynomial) as possible and the actual attacking or *online phase* where the attacker solves the system of linear equations.

APPLICATION

During our investigation, we adopted Armknecht and Krause's approach in order to model the E0 encryption function, so that we are not to be dependent on memory bits and which will hold for every clock tick. We came up with a polynomial of degree four consisting of twenty variables, sixteen considered unknown and four known; the details are available in [7].

We then created an automated tool in the Maple 12 environment (http://www.maplesoft.com) that finds all of the maxterms and their corresponding superpolys (linear coefficients) for the E0 encryption function. The most time-consuming work in the computation process, finding the maxterms and their corresponding superpolys, was executed in the Maple 12 environment because we wanted to benefit from the advantages of a high-performance mathematical engine with a fully integrated algebraic processing system.

In the online phase, we used a chosen plaintext attack to solve the system of 12 linear equations by 8 unknowns we found. Part of the cube attack is a chosen plaintext attack – the part that can be manipulated by the attacker. In order to implement the cube attack we assume that the attacker has the capability of sending properly structured packets that the Bluetooth receiver will

respond to, thus providing the attacker with access to the encryption machine.[1] Note that the encryption machine behaves like an oracle. If the attacker convinces the Bluetooth oracle that he or she is a legitimate participant then the oracle will be duped into sending data to the attacker or another participant; however, the attacker can observe "over the air," whatever responses the oracle or the user sends back. For instance, the attacker can masquerade as a real user, with sufficient detail, so that he can send data to the oracle. The oracle will send encrypted data back to the attacker or to an authorized user/participant in the communication process and the attacker will collect this data. The attacker will gain some knowledge of the output bitstreams of the combiner at clock times *t, t+1, t+2*, *and t+3*. More formally, we proved in [7] that assuming that an attacker has unauthorized access to the encryption protocol, then by knowing the output bitstream at any clock time, the cube attack as we have modeled it, is successful in recovering the outputs of the LFSRs of the E0 keystream generator at *any* stage.

RESULTS

Using the Maple program, we found twelve superpolys, including the unknown variables of the 4 LFSRs for two consecutive clock times. The program was executed on an Intel Pentium 4 processor with a CPU of 2.80Ghz and 1GB of RAM, and the results were produced in 8.03 seconds, consuming 5.25 MB of memory.

From the specific encryption function of the multivariable polynomial (obtained after the attacker masquerades as an authorized user and gains access to the security protocol), the attacker will eventually succeed in gathering twelve unique and independent equations, solve them using a chosen plaintext attack and recover the output bits of the LFSRs.

[1] This is not quite as easy to do in Bluetooth as it is with, say, 802.11 based system, but can be accomplished with some work.

We measured the complexity of the steps. During the preprocessing phase an attacker tries to find as many maxterms as possible. From this phase, an attacker may obtain *n+1* output bits from the LFSRs and some constant terms. The amount of work needed, based on the analysis in [8] is

$$n(n+1)2^{d-1},$$

where *d* as the degree of the encryption function *f* and *n* as the number of variables. The attacker also needs to compute the inverse of the matrix of linear relations. This produces an upper bound from this phase of

$$n(n+1)2^{d-1}+n^3$$

For the online phase, in which it is necessary to solve the system of linear equations implementing a chosen plaintext attack, $n2^{d-1}$ evaluations of the E0 encryption function are needed, and the matrix multiplication which takes n^2 operations needs to be performed. Again, using the analyses described in [1, 8] we deduce a complexity of

$$n2^{d-1}+n^2$$

Therefore, the overall complexity from both phases is as follows:

$$n(n+1)2^{d-1}+n^3+n2^{d-1}+n^2=$$
$$n^2 2^{d-1}+2n2^{d-1}+n^3+n^2$$

which is equivalent to $O(n^2 2^{d-1}+n^3)$.

In the case of Bluetooth with *n=128 and d=4*, we determine that the attack on E0 requires

$$2246656 \approx 2^{21.1}$$

bit operations.

The number of operations needed in the computational process is considerably less than that of similar algebraic types of attacks described in [3]-[6], but it is limited to the output of the LFSRs at any clock tick. Further insight is necessary

Comment [npetrako1]: I include the correlation attacks also, if only the algebraic then it is [3],[4]

to reveal the encryption key having the output of every LFSR at any time. This raises the question: given the output of the LFSRs how do we find the key?

Building on these results, the next stage of the research is to validate our integration of the cube-type attack into the Bluetooth encryption protocol. As demonstrated in this and other research we cited one needs to be able to understand and formally evaluate the strengths of a given cryptosystem and be able to evaluate the implementation of the cryptosystem to ensure that there are no flaws in the application of the cryptosystem. The cryptosystem and the protocol it uses may be good but if poorly implemented will most likely be untrustworthy.

ABOUT THE AUTHORS

George Dinolt is an Associate Professor in the Computer Science Department at the Naval Postgraduate School. His research interests are primarily in the "high assurance" portions of Computer Security. He works in Formal Methods and the connections between them and Security Policies, Secure Systems Architectures and Secure Systems Design. He also works in Computer Network (Cyber) Operations. Contact him at gwdinolt@nps.edu.

James Bret Michael is a Professor in the Computer Science Department at the Naval Postgraduate School. His research interests are in the reliability, safety, and security of distributed systems, computer-aided formal verification and validation of systems, and system of systems engineering. Contact him at bmichael@nps.edu.

Pantelimon Stanica is an Associate Professor in the Department of Applied Mathematics at the Naval Postgraduate School. His research interests are in Cryptography & Coding theory, Boolean Functions, Logic and Discrete Mathematics, Number Theory, Graph Theory, Combinatorial Mathematics, Algebra. Contact him at pstanica@nps.edu.

Nikolaos Petrakos is an officer of the Hellenic Navy. He received his bachelor from the Hellenic Naval Academy in 1996. Petrakos received his master degrees in Computer Science and in Applied Mathematics from the Naval Post Graduate School in 2009. Contact him at npetrako@gmail.com.

REFERENCES

[1] I. Dinur and A. Shamir, *Cube Attacks on Tweakable Black Box Polynomials*, in Proceedings of the 28th Annual International Conference on Advances in Cryptology: The Theory and Applications of Cryptographic Techniques, LNCS 5479, Springer, 2009, pp. 278-299.

[2] S. Fischer, S. Khazaei, and W. Meier, *Reduced Complexity Attacks on the Alternating Step Generator*, in Proceedings of Selected Areas in Cryptography, LNCS 4876, Springer, 2007, Springer, 2007, pp. 1-16.

[3] F. Armknecht, M. Krause, Algebraic Attacks on Combiners with Memory, lecture notes, unpublished, http://cat.inist.fr/?aModele=afficheN&cpsidt=15690405, last accessed Feb. 2009.

[4] F. Armknecht, *Algebraic Attacks on Stream Ciphers*, in Proceedings of the European Congress on Computational Methods in Applied Sciences and Engineering, 2004.

[5] Y. Lu, S. Vaudenay, *Faster Correlation Attack on Bluetooth Keystream Generator E0*, in Advances in Cryptology - CRYPTO 2004, 24th Annual International Cryptology Conference, LNCS 3152, Springer, 2004, p. 407-425.

[6] Y. Lu, W. Meier, S.Vaudenay, *The Conditional Correlation Attack: A Practical Attack on Bluetooth Encryption*, in Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference, LNCS 3621, Springer, 2005, pp. 97-117.

[7] N. Petrakos, ,Cube-type Algebraic Attacks on Wireless Encryption Protocols, Master's Thesis, Naval Postgraduate School, Monterey, CA, Sept. 2009.

[8] A. Zhang, C.-W. Lim and K. Khoo, *Extensions of the Cube Attack*, Cryptology ePrint Archive, Report 2009/049, 2009. http://eprint.iacr.org/.